(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 779 570 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.06.1997 Bulletin 1997/25

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **96308205.2**

(22) Date of filing: **13.11.1996**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **11.12.1995 US 570463**

(71) Applicant: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Kells, Timothy Roger**
  Round Rock, Texas 78681 (US)
- **Peebles, Thomas Frank**
  Austin, Texas 78758 (US)

(74) Representative: **Zerbi, Guido Maria**
Intellectual Property Department,
IBM United Kingdom Ltd.,
Hursley Park
Winchester, Hampshire SO21 2JN (GB)

(54) System and method for supporting distributed computing mechanisms in a local area network server environment

(57) LAN server machines are configured to utilize their existing mechanisms to pass generic security subsystem (GSS) distributed computing environment (DCE) credentials. The server management block (SMB) protocol is extended to facilitate exchange of such credentials wherein the server utilizes the GSS API interface to obtain and validate such credentials. The GSS interface provides tokens which encapsulate all necessary information to perform mutual authentication between the client and server.

A new protocol level is defined with respect to such SMB protocol extensions which includes a new protocol name exchanged in the negotiate protocol (NP) SMB. Pre-existing LAN servers will turn on a bit in the SMB_Secmode field in the NP response indicating that the server supports exchange of secpkgX SMB. The server will then wait for an SMB secpkgX or SMB sess-setupX response. The former response will permit the user/client and server to exchange GSS tokens utilizing a conventional LAN server mechanism and to thereby and mutually authenticate.

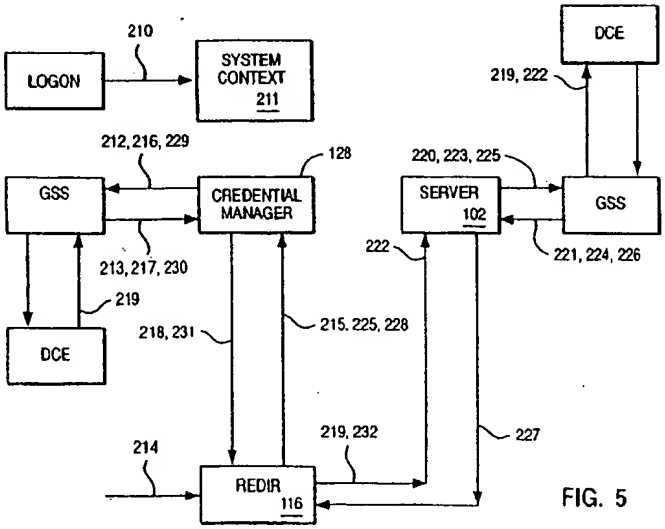


FIG. 5

EP 0 779 570 A1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 942 568 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.09.1999 Bulletin 1999/37

(51) Int Cl.[6]: **H04L 29/06**

(21) Application number: **99301079.2**

(22) Date of filing: **15.02.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **17.02.1998 US 24928**

(71) Applicant: **Unwired Planet, Inc.**
Redwood City, California 94063 (US)

(72) Inventor: **Ramasubramani, Seetharaman**
San Jose, CA 95129 (US)

(74) Representative: **Suèr, Steven Johannes et al**
Ablett & Stebbing,
Caparo House,
101-103 Baker Street
London W1M 1FD (GB)

(54) Centralized cerificate management system for two-way interactive communication devices in data networks

(57) The present invention discloses a method for managing centralized certificates in a proxy server device (114) for a plurality of thin client devices (302, 304, 306) coupled thereto through a data network (102). A user account database, accessible by the proxy server, comprises a plurality of user accounts with each of the thin client devices being associated with one or more of the user accounts. Each of the user accounts comprises a device ID (316), a list of public and private keys (326) assigned to the user account, and a list of certificates (320) assigned to the user account. A certificate management module reserves a fixed number of free certificates signed by a Certificate Authority and their respective private keys in a certificate database (328) and frequently updates the free certificate according to a certificate updating message. Whenever a user account is created for a thin client device, the certificate management module fetches one or more free certificates from the certificate database and associates the fetched certificate(s) to the created account and at the same time creates new free certificates with the Certificate Authority to fill in the certificate database.

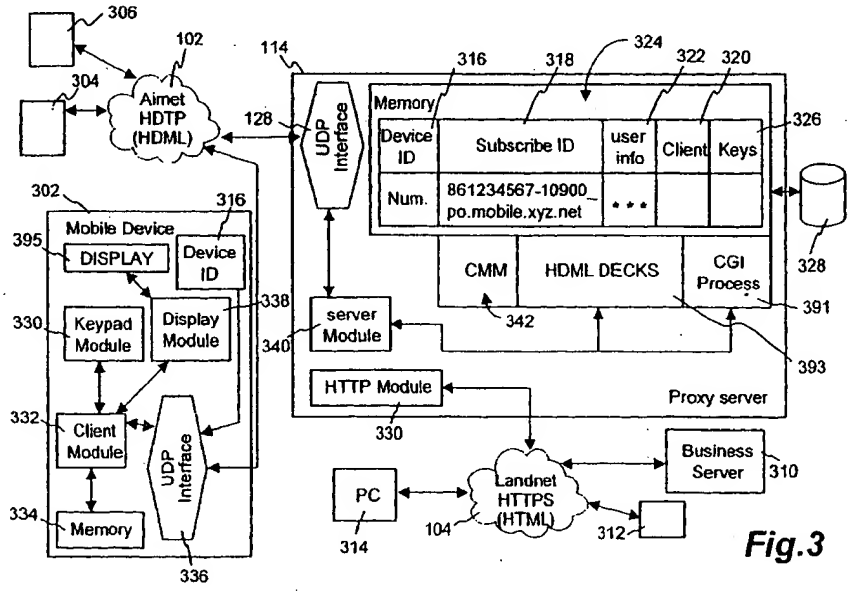


Fig.3

EP 0 942 568 A2

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, G06F 12/14, 1/00 — A1

(11) International Publication Number: WO 99/41878

(43) International Publication Date: 19 August 1999 (19.08.99)

(21) International Application Number: PCT/US99/03311

(22) International Filing Date: 17 February 1999 (17.02.99)

(30) Priority Data:
60/078,848 17 February 1998 (17.02.98) US

(71) Applicant: AT & T CORP. [US/US]; 32 Avenue of the Americas, New York, NY 10013-2412 (US).

(72) Inventors: BLAZE, Matthew, A.; P.O. Box 1873, Hoboken, NJ 07030 (US). FEIGENBAUM, Joan; 148 W. 23rd Street, 2A, New York, NY 10011 (US). STRAUSS, Martin, J.; 25 Hickory Place #D-2, Chatham, NJ 07928 (US).

(74) Agent: DWORETSKY, Samuel, H.; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).

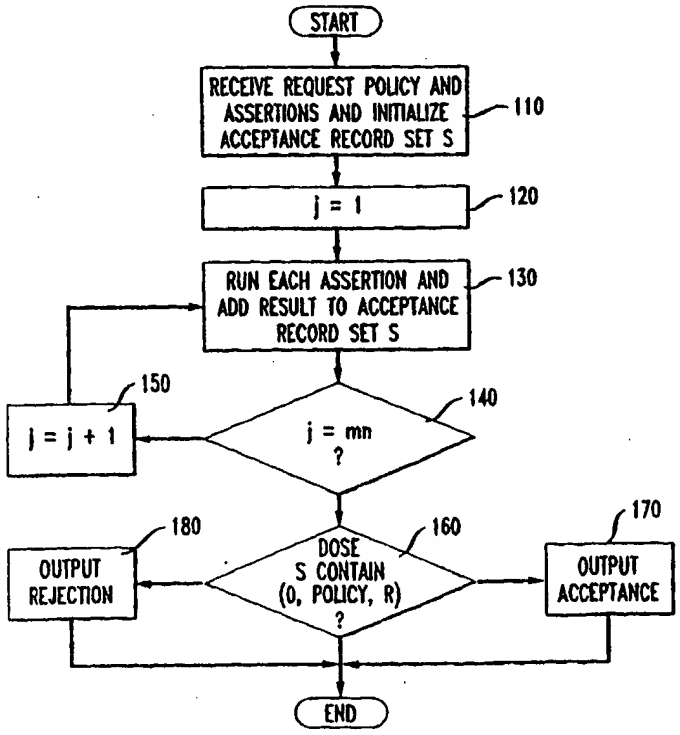
(81) Designated States: CA, JP, MX, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR COMPLIANCE CHECKING IN A TRUST-MANAGEMENT SYSTEM

(57) Abstract

A method and apparatus are provided for compliance checking in a trust-management system. A request r, a policy assertion (f_0, POLICY), and $n-1$ credential assertions (f_1, s_1), ..., (f_{n-1}, s_{n-1}) are received, each credential assertion comprising a credential function f_i and a credential source s_i. Each assertion may be monotonic, authentic, and locally bounded. An acceptance record set S is initialized to {(Λ, Λ, R)}, where Λ represents a distinguished null string, and R represents the request r. Each assertion (f_i, s_i), where i represents the integers from $n-1$ to 0, is run and the result is added to the acceptance record set S. This is repeated mn times, where m represents a number greater than 1, and an acceptance is output if any of the results in the acceptance record set S comprise an acceptance record (0, POLICY, R).



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2001 (18.10.2001)

PCT

(10) International Publication Number
WO 01/077797 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/11907

(22) International Filing Date: 11 April 2001 (11.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/547,183 11 April 2000 (11.04.2000) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS PALI-521, Palo Alto, CA 94303 (US).

(72) Inventors: ELLEY, Yassir, K.; 664 B South Street, Waltham, MA 02453 (US). ANDERSON, Anne, H.; 28 Minuteman Road, Acton, MA 01720 (US). HANNA, Stephen, R.; 3 Beverly Road, Bedford, MA 01730 (US). MULLAN, Sean, J.; 102 Ashbrook, Howth Road, Clontarf, Dublin 3 (IE). PERLMAN, Radia, Joy; 10 Huckleberry Lane, Acton, MA 01720 (US).

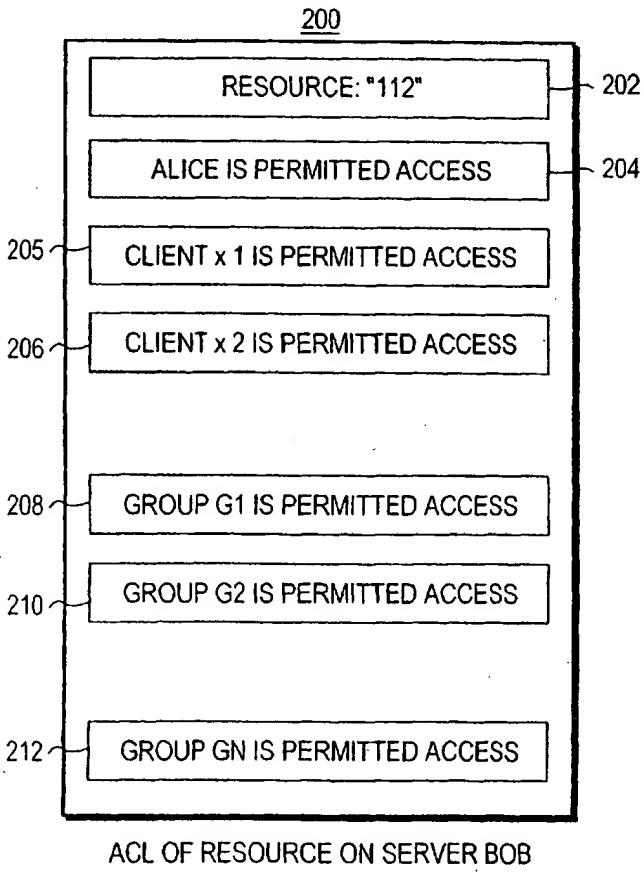
(74) Agents: CESARI, Robert, A. et al.; Cesari and McKenna, LLP, 88 Black Falcon Avenue, Boston, MA 02210 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR MANAGING CREDENTIALS



ACL OF RESOURCE ON SERVER BOB

(57) Abstract: The basic concept is that before a resource is accessed, the entity that has the burden of gathering the credentials, pro-actively refreshes the credentials and keeps them current. In one instance, a presenter of credentials, for example, a client pro-actively refreshes the credentials such that at the time of presentation, the credentials meet the resource-specific constraints of a recipient of credentials, for example, a resource server. For each resource that it protects, a resource server typically establishes various constraints such as a recency requirement, which specifies how recently a credential has to have been issued to be accepted as an adequate credential. Other constraints may include maximum certificate chain length, trust level and so forth. In another instance, a recipient of credentials pro-actively gathers and refreshes credentials to prevent un-authorized access to the various resources it is protecting.

WO 01/077797 A3